APPENDIX A — OPINION AND JUDGMENT OF THE UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT DATED AND DECIDED SEPTEMBER 17, 2001

UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT

00-1373, 00-1374

September 17, 2001, Decided

HILGRAEVE CORPORATION,

Plaintiff-Appellant,

v.

SYMANTEC CORPORATION,

Defendant-Cross Appellant.

* * *

JUDGES:

Before RADER, Circuit Judge, PLAGER, Senior Circuit Judge, and DYK, Circuit Judge.

OPINION

DYK, Circuit Judge.

Hilgraeve Corp. ("Hilgraeve") appeals from the decision of the United States District Court for the Eastern District of

Appendix A

Michigan granting the motion of Symantec Corp. ("Symantec") for summary judgment of non-infringement for U.S. Patent No. 5,319,776 (" '*776* Patent"). *Hilgraeve Corp. v. Symantec Corp.*, 90 F. Supp. 2d 850 (E.D. Mich. 2000). Symantec cross-appeals the district court's grant of summary judgment for Hilgraeve that Symantec is not licensed to use the invention claimed in the '*776* Patent. *Hilgraeve Corp. v. Symantec Corp.*, Civ. Action No. 97-40370 (E.D. Mich. Jun. 28, 1999) ("License Defense Order").

We vacate the district court's grant of summary judgment of non-infringement of the '*776* Patent and generally affirm the district court's grant of summary judgment that Symantec did not license the '*776* Patent. We find that questions of material fact exist as to whether the limitations of the '*776* Patent claims are found in the methods performed by the accused products, and that Hilgraeve did not transfer any rights to practice the '*776* Patent.

BACKGROUND

Hilgraeve filed suit against Symantec in the Eastern District of Michigan for infringement of the '*776* Patent on September 15, 1997. On the same day, Hilgraeve filed a separate suit against McAfee Associates, Inc. for infringement of the '*776* Patent, also in the Eastern District of Michigan. The cases were not consolidated. In the McAfee case, the district court's grant of summary judgment of non-infringement, *Hilgraeve Corp. v. McAfee Associates, Inc.*, 70 F. Supp. 2d 738 (E.D. Mich. 1999) ("McAfee I "), was vacated and remanded by this court because, under the agreed claim construction, questions of material fact existed about

the operation of the accused device, 224 F.3d 1349, 55 USPQ2d 1656 (Fed. Cir. 2000) ("McAfee II "). The '*776* Patent relates to computer virus detection software. The software scans a digital data file for viruses as the file is transferred to a storage medium. If the software detects a virus prior to storing the file, it automatically blocks storage of the file. The software may be used, for example, to scan a file for viruses as the file is transferred from a floppy disk to a hard disk of a computer system, or as the file is transferred over the Internet from one computer system to a storage medium of another computer system.

The '*776* Patent contains 20 claims. Independent claims 1 and 18, which are at issue on this appeal, read as follows:

> 1. In a system for transferring digital data for storage in a computer storage medium, a method of screening the data as it is being transferred and automatically inhibiting the storage of screened data containing at least one predefined sequence, comprising the steps of:
>
> causing a quantity of digital data resident on a source storage medium to be transferred to a computer system having a destination storage medium;
>
> receiving and screening the transferred digital data prior to storage on the destination storage medium to determine if at least one of a plurality of predefined sequences are present in the digital data received; and
>
> in response to said screening step:

Appendix A

(a) automatically causing the screened digital data to be stored on said destination storage medium if none of the plurality of predefined sequences are present, and

(b) automatically inhibiting the screened digital data from being stored on said destination storage medium if at least one predefined sequence is present.

18. A method of preventing the spread of computer viruses to a computer having a storage medium, comprising the steps of:

simultaneously searching for a plurality of virus signatures, each of which comprising an identifiable digital sequence, while said computer is receiving a stream of digital data for storage on said storage medium;

providing an indication of the detection of a virus from said searching step; and

automatically inhibiting the storage of said digital stream on said storage medium if any of said virus signatures have been detected.

'*776* Patent, col. 17, ll. 9-29 and col. 18, ll. 45-57 (emphases added to pertinent terms).

Because these claims require the inhibition of "storage," the district court was required to construe the meaning of

the word "storage" in the patent. The district court construed "storage" as occurring "when the incoming digital data is sufficiently present on the destination storage medium so that any viruses contained in the data can spread and infect the computer system." *Hilgraeve*, 90 F. Supp. 2d at 857.

Hilgraeve contended that several Symantec products, including pcANYWHERE TM and Norton Antivirus TM ("NAV"), infringe the *'776* Patent under this claim construction. In other words, Hilgraeve alleged that the accused products screen incoming digital data for viruses during transfer and before "storage" on the destination storage medium. In contrast, Symantec contended that its products do not infringe because they screen for viruses only after the data have been "stored" on the destination storage medium. Thus, the critical issue was whether the accused products screen for viruses before or after the data become sufficiently present on the storage medium so that viruses contained in the data could spread and infect the computer system.

To resolve this issue on summary judgment the district court relied on testimony of Symantec's expert witness about how the accused products operate and on statements made by Hilgraeve and its expert that it agreed with the overview offered by Symantec's expert about how the accused products operate. *Hilgraeve*, 90 F. Supp. 2d at 858-59. Upon accepting Symantec's view of how the products operate, the district court found that the accused products "first allow the incoming digital data to be stored as a whole on the destination storage medium before it is scanned. Virus screening is performed only after the incoming digital data has been fully transferred and stored." *Id.* at 859. The district

court held that "[b]ecause there is no dispute about how the accused products operate, there is no genuine issue as to any material fact concerning whether Defendant's accused products literally infringe the *'776* Patent" and granted summary judgment for Symantec. *Id.*

Before the district court, Symantec also asserted the affirmative defense to Hilgraeve's infringement claim that it had acquired a license to use the patent under a complex series of transactions involving Delrina Corp. and its subsidiaries. On June 30, 1993, Delrina Corp., Delrina (Delaware) (a subsidiary of Delrina Corp.), and Hilgraeve executed a Technology Transfer Agreement under which Delrina Corp. paid Hilgraeve $1.45 million, and Hilgraeve transferred certain rights to its software, allegedly including the technology at issue in this suit, to Delrina (Delaware). The Technology Transfer Agreement states that it is governed by the laws of the Province of Ontario, Canada. On the same day, Delrina (Canada) (also a subsidiary of Delrina Corp.) and Delrina (Delaware) entered into a Software Development and Cost Sharing Agreement (the "SDCS Agreement") to govern the shared development of software by the parties. In July 1995, Symantec acquired Delrina Corp. On March 30, 1996, Delrina (Canada) licensed its intellectual property to Symantec. On March 2, 1999, Delrina (Delaware) entered into an agreement with Symantec to directly transfer rights to the technology transferred by Hilgraeve to Delrina (Delaware) on June 30, 1993.

The district court granted Hilgraeve's motion for summary judgment that Symantec did not have a license to the *'776* Patent prior to March 2, 1999, because Symantec

had failed to establish that Delrina (Delaware) transferred any rights to the '*776* Patent to Delrina (Canada) or Delrina Corp., and Symantec therefore failed to show that it acquired any rights to the '*776* Patent through the 1995 acquisition of Delrina Corp. License Defense Order, slip op. at *14. As to events after March 2, 1999, the district court denied both Hilgraeve's and Symantec's motions for summary judgment regarding Symantec's licensing defense, finding that the March 2, 1999, agreement raised a general issue of material fact as to whether Symantec had acquired a license to the '*776* Patent through the March 2, 1999 agreement. *Id.* After granting Symantec's motion for summary judgment of non-infringement, the district court denied all other pending motions in the case without prejudice, and dismissed the case. *Hilgraeve*, 90 F. Supp. 2d at 859.

DISCUSSION

I. Jurisdiction and Standard of Review

We have jurisdiction over this appeal pursuant to 28 U.S.C. § 1295(a)(1). Summary judgment is properly granted when "there is no genuine issue as to any material fact and . . . the moving party is entitled to a judgment as a matter of law." Fed. R. Civ. P. 56(c); *Chiuminatta Concrete Concepts, Inc. v. Cardinal Indus., Inc.*, 145 F.3d 1303, 1307, 46 USPQ2d 1752, 1755 (Fed. Cir. 1998). We review a district court's grant of a motion for summary judgment without deference. *Ethicon Endo-Surgery, Inc. v. United States Surgical Corp.*, 149 F.3d 1309, 1315, 47 USPQ2d 1272, 1275 (Fed. Cir. 1998).

Appendix A

A patent infringement analysis requires two steps. *Gentry Gallery, Inc. v. Berkline Corp.*, 134 F.3d 1473, 1476, 45 USPQ2d 1498, 1500 (Fed. Cir. 1998). "First, the claim must be properly construed to determine its scope and meaning. Second, the claim as properly construed must be compared to the accused device or process." Id. (quoting *Carroll Touch, Inc. v. Electro Mech. Sys., Inc.*, 15 F.3d 1573, 1576, 27 USPQ2d 1836, 1839 (Fed. Cir. 1993)). Claim construction is a matter of law that is reviewed without deference. *Cybor Corp. v. FAS Techs., Inc.*, 138 F.3d 1448, 1456, 46 USPQ2d 1169, 1174 (Fed. Cir. 1998) (en banc). Determination of infringement, whether literal or under the doctrine of equivalents, is a question of fact. *Bai v. L & L Wings, Inc.*, 160 F.3d 1350, 1353, 48 USPQ2d 1674, 1676 (Fed. Cir. 1998). "Thus, summary judgment of non-infringement can only be granted if, after viewing the alleged facts in the light most favorable to the non-movant, there is no genuine issue whether the accused device is encompassed by the claims." *Pitney Bowes, Inc. v. Hewlett-Packard Co.*, 182 F.3d 1298, 1304, 51 USPQ2d 1161, 1165 (Fed. Cir. 1999).

We review the construction of a license agreement without deference and interpret the licensing agreement under the law governing the agreement, here Ontario law. See Studiengesellschaft Kohle, m.b. *H. v. Hercules, Inc.*, 105 F.3d 629, 632, 41 USPQ2d 1518, 1521 (Fed. Cir. 1997) (citing *Cyrix Corp. v. Intel Corp.*, 77 F.3d 1381, 1384, 37 USPQ2d 1884, 1887 (Fed. Cir. 1996)).

Appendix A

II. Claim Construction Issues

As noted above, this is our second case involving the '*776* Patent. In McAfee II, we accepted the claim construction of "storage" urged by both parties and adopted by the district court in McAfee I. That claim construction differs slightly from the claim construction adopted below in the district court in this case in that the McAfee II claim construction views "storage" as occurring "when the incoming digital data is sufficiently present on the destination storage medium, and accessible by the operating system or other programs, so that any viruses contained in the data can spread and infect the computer system." *McAfee II*, 224 F.3d at 1351 (emphasis added to differing language).

Symantec argues that "storage" should not be construed to occur when data become "accessible by the operating system or other programs," *Hilgraeve*, 90 F. Supp. 2d at 857, or when "any viruses contained in the data can spread and infect the computer system," but that "storage" should be construed to occur when the data become physically present (i.e., magnetically recorded) on the storage medium.

We need not decide here whether our claim construction in McAfee II is binding on us in this case as a matter of stare decisis. Our decision in McAfee II was precedential, but it merely adopted the district court's claim construction in McAfee I based on the parties' agreement that the district court's claim construction was correct. We have independently considered the issues of claim construction and conclude that the construction of "storage" in McAfee II is indeed correct.

Appendix A

The '*776* Patent distinguishes prior art virus scanning programs because they "do not automatically prevent the virus from being stored on the medium in the first place, hence they cannot totally prevent the virus from attacking or spreading." '*776* Patent, col. 1, ll. 51-54. Thus, "storage" of the virus is identified with the virus's ability to spread and infect the computer system. A virus may not spread or infect the computer system, however, unless it is accessed by the operating system or other programs. Given this, we agree with the McAfee II court that "storage" occurs "when the incoming digital data [are] sufficiently present on the destination storage medium and accessible by the operating system or other programs so that any viruses contained in the data can spread and infect the computer system."[1] *McAfee II*, 224 F.3d at 1351.

III. Infringement

Symantec contends that even under our claim construction it does not infringe. Hilgraeve argues that questions of material fact remain regarding the operation of the accused devices and hence infringement.[2] We conclude here that the conflicting

1. The parties also dispute whether "destination storage medium" as used in claim 1 and "storage medium" as used in claim 18 mean the ultimate destination of the digital data or whether the terms may be construed to include an intermediate storage medium. In accordance with the definition of "storage" we have adopted, we conclude that "storage medium" refers to any storage medium of the computer system, if the data, when stored on the medium, are accessible to the operating system or other programs, such that viruses in the data can spread and infect the computer system.

2. While the parties, and the district court's decision, speak of the accused devices as infringing, more properly the allegation is

(Cont'd)

affidavits of the parties' experts leave material fact questions unanswered, just as we held in a somewhat similar context in McAfee II.

The district court based its summary judgment of non-infringement on the testimony of Symantec's expert, Dr. Melvin, who opined on the operation of the accused products, and on statements made by Hilgraeve and its expert, Dr. Geske, agreeing with portions of Dr. Melvin's testimony. The experts, however, did not in fact agree.

The experts described the operation of the accused products in different ways. Symantec's expert, Dr. Melvin, described the operation of NAV as occurring in a sequence of steps. In this sequence, first (step one) a file is transferred for storage onto the destination storage medium. This transfer includes opening a new file on the storage medium and recording incoming data into the new file. Second (step two), the application causing the transfer makes a request to the operating system to close the file containing the transferred data. Third (step three), the operating system closes the file. Fourth (step four), after the file is closed, the Symantec product invokes the NAV Scan Engine to test the file for the presence of a virus. Symantec's expert alleged that after the third step and before the fourth step, the file is recorded on the storage medium and accessible to the operating system and other programs – and therefore "stored," and that since this occurs before the file is scanned for viruses, Symantec's

---

(Cont'd)

that the operation of the devices directly infringes the method claims at issue, or that the sale of the devices induces customers to infringe the method claims.

products do not infringe. Hilgraeve's expert, Dr. Geske, stated that although he agreed with Dr. Melvin's "overview" of how the accused products operate, in his opinion there were critical points in Dr. Melvin's analysis that did not correspond with the behavior of the NAV as it executes. Critically, Dr. Geske interpreted the testimony of Mr. Cohen, the Chief Architect of the Symantec accused products, to mean that the accused products impose a barrier in the computer system's file system which prevents all programs and the operating system from accessing the transferred file until it is processed and screened for viruses. Thus, Dr. Geske disputed that the file becomes accessible to the operating system and other programs between steps three and four.

Symantec's expert sought to prove that a file becomes accessible to the operating system or other programs before it is scanned for viruses by the NAV Scan Engine by running four tests. Hilgraeve's expert asserted that these tests do not prove that Symantec's products do not infringe, and that even if they showed that the products do not infringe under the test circumstances, they do not prove non-infringement under normal operating conditions.

We agree that tests of an accused device under unusual conditions are not necessarily relevant to an infringement analysis. For example, in determining whether a product claim is infringed, we have held that an accused device may be found to infringe if it is reasonably capable of satisfying the claim limitations, even though it may also be capable of non-infringing modes of operation. *See Intel Corp. v. United States Int'l Trade Comm'n*, 946 F.2d 821, 832, 20 USPQ2d 1161, 1171 (Fed. Cir. 1991); *Key Pharms., Inc. v. Hercon Labs. Corp.*, 981 F. Supp. 299, 310 (D. Del. 1997), *aff'd*,

161 F.3d 709, 48 USPQ2d 1911 (Fed. Cir. 1998); *Huck Mfg. Co. v. Textron, Inc.*, 1975 U.S. Dist. LEXIS 12539, 187 USPQ 388, 408 (E.D. Mich. 1975) ("The fact that a device may be used in a manner so as not to infringe the patent is not a defense to a claim of infringement against a manufacturer of the device if it is also reasonably capable of a use that infringes the patent."); cf. *High Tech Med. Instrumentation, Inc. v. New Image Indus., Inc.*, 49 F.3d 1551, 1556, 33 USPQ2d 2005, 2009 (Fed. Cir. 1995) (finding that an accused device does not infringe if it does not infringe in its normal configuration, even if it may be altered into an infringing configuration under unusual circumstances). So too the sale of a device may induce infringement of a method claim, even if the accused device is capable of non-infringing modes of operation in unusual circumstances.

In the first test, Symantec's expert downloaded an infected file from a web page on the Internet to a storage disk of a computer running NAV and the Windows 95 TM operating system. After the file arrived at the computer, but before the NAV was able to scan and delete the file, he shut off power to the computer. When he turned the computer on again he was able to access the file with a utility program of Windows 95. In the second test, Dr. Melvin also downloaded an infected file from a web page to a storage disk of a computer running NAV, but he restarted the computer instead of shutting off its power, prior to scanning by NAV. When the computer restarted, he was able to access the file. Symantec alleges that these two tests show that the file is stored on the computer's storage medium prior to scanning. Even if that is true as a factual matter under the circumstances of the tests, the tests are not probative of infringement during normal operation of the accused products. Because the '*776*

Patent claims require "automatically inhibiting" the storage of the virus, as we said in McAfee II when considering similar tests, "a test disabling the automatic capabilities of [the accused product] is not probative of whether [the accused product] may infringe in the automatic mode." *McAfee II*, 224 F.3d at 1354.

In Dr. Melvin's third test, he downloaded an infected file to a computer running both NAV and McAfee's anti-virus screening program, VirusScan TM. VirusScan intercepted and examined the file before NAV screened it for viruses, which according to Dr. Melvin, showed that the file was accessible by other programs prior to screening by NAV. While this third test may demonstrate that the infected file is accessible to VirusScan before it is screened by NAV, it is not clear from this test that the virus can spread and infect the computer system before it is screened by NAV, especially since both NAV and VirusScan are intended to prevent the spread of viruses. Moreover, as with the first two tests, whether or not the accused products infringe when operated in conjunction with another anti-virus product — perhaps an unusually redundant mode of operation — does not answer the question whether they infringe while operating alone.

In his fourth test, Dr. Melvin loaded into memory NAV and a special program for intercepting a particular file while the file is being downloaded and redirecting the file to the computer's storage medium. When Dr. Melvin then downloaded the particular file, which contained a virus, it was intercepted and redirected to the storage medium by the special program before it could be screened by NAV for viruses. That this test may prove that the functionality of the

accused products can be defeated to avoid infringement does not prove non-infringement of the products under normal operating conditions.

Thus, we find the tests inconclusive on the issue of infringement. Because the record shows the existence of genuine issues of material fact concerning the interaction of the accused devices with the operation system and other programs, the district court erred in granting summary judgment of non-infringement.

IV. Symantec's Licensing Defense

Symantec urges that even if we vacate the district court's grant of summary judgment of non-infringement, the judgment can be affirmed on an alternative ground, namely that Symantec was licensed to practice the patent. We cannot agree.

The district court held that Symantec had no license defense for the period prior to March 2, 1999, because the purported transfer of patent rights from Delrina (Delaware) to Delrina (Canada) under the June 30, 1993 SDCS agreement was ineffective. While the district court appears to have been correct, we believe that there is a more fundamental defect in Symantec's license defense argument – Delrina (Delaware) itself never acquired a transferable license to practice the '*776* Patent, and Delrina (Delaware) therefore could not sub-license the '*776* Patent either before March 2, 1999, or thereafter.

Appendix A

Unless the '*776* Patent was licensed under the June 30, 1993 Agreement, Symantec agrees that it could not acquire a license. Symantec also admits that there is no express language in the June 30, 1993 Technology Transfer Agreement licensing or transferring rights to the '*776* Patent or any other Hilgraeve patent. Instead, Symantec points to language in the paragraph 2.1 of the Agreement providing that "HILGRAEVE sells, conveys, assigns and transfers to DELRINA DELAWARE and to HILGRAEVE, as joint tenants and not as tenants in common, all copyright rights in the Software," and that Hilgraeve acknowledged in paragraph 9.1 that as part of the transfer "HILGRAEVE has also agreed to transfer the necessary know-how and technical expertise to DELRINA DELAWARE with respect to the Software." On the basis of this language, Symantec urges us to find that:

> 'Software' is more than source code and object code. . . . When read in conjunction with the . . . 'know-how' and 'technical expertise' transferred to Delrina (Delaware), Delrina (Delaware) essentially acquired Hilgraeve's entire knowledge base with respect to [Hilgraeve's] products. Since the Software included in-transit anti-virus features, Delrina acquired Hilgraeve's knowledge base with respect to those in-transit anti-virus features and could use that knowledge base as it pleased.

In summary, Symantec urges us to find that "the Technology Transfer Agreement covered the technology in this case, which is allegedly covered by the '*776* Patent."

Appendix A

Whatever the definition of "knowledge base" proposed by Symantec, we cannot conclude that rights to the *'776* Patent were transferred by the Technology Transfer Agreement. Under Ontario law, "effect must first be given to the intention of the parties, to be gathered from the words they have used. . . ." *Consol. Bathurst Exp. Ltd. v. Mut. Boiler & Mach. Ins. Co.*, 1 S.C.R. 888, 888 (Can. 1980). When the language of a contract is clear and unambiguous, only the contract is considered for interpretation, not extrinsic evidence. *Indian Molybdenum v. The King*, 3 D.L.R. 497, 502 (Can. 1951). Here, the contract provided for Hilgraeve to transfer "all copyright rights in the Software," but failed to mention the transfer of patent rights. From the terms of the contract we cannot conclude that the parties intended to transfer any patent rights. Symantec relies on *Allan v. Bushnell T.V. Co., Ltd.*, 1 D.L.R. (3d) 534, 539 (Ont. High Ct. 1968) for the proposition that "unexpressed terms [are implied] to implement [the] parties' presumed intention." Allan, however, stated that

> the presumption is against the adding to contracts of terms which the parties have not expressed. The general presumption is that the parties have expressed every material term. . . . But . . . there may be cases where obviously some term must be implied if the intention of the parties is not to be defeated, some term of which it can be predicated that 'it goes without saying', some term not expressed but necessary to give to the transaction such business efficacy as the parties must have intended.

Id. Allan was a case involving a contract between a broadcasting company and a news service in which the unexpressed term

which was implied in the contract was that the news to be supplied to the company by the service had to be "accurate." Here, we cannot say (and it does not "go without saying") that where the contract provided for the transfer of copyrights in the software, but failed to mention the transfer of patent rights, that we must imply such a term to the contract. The contract has a business efficacy without adding this unexpressed term to it.

Moreover, in the subparagraph immediately following the paragraph 2.1 pertaining to the transfer of copyrights, the contract refers to other intellectual property rights. In paragraph 2.2, the parties agreed that Hilgraeve "shall not assert against DELRINA DELAWARE, any other intellectual property right, including patent rights, it has or may have in the future, with respect to the production, copying, licensing of the Software, or the exercise by DELRINA DELAWARE of any rights transferred hereunder." Since the contract specifically mentions patent rights in paragraph 2.2, we cannot say that the omission of mention of patent rights in paragraph 2.1, which transferred rights to copyrights in the Software, was accidental or that the transfer of patent rights is implicit anywhere the contract. *Cf. State Contracting & Eng'g Corp. v. Florida*, 258 F.3d 1329, 59 USPQ2d 1498 (Fed. Cir. 2001) (applying Florida law to construe an agreement).

Symantec also contends that the covenant not to sue for patent infringement in paragraph 2.2 is equivalent to a freely transferable license to the patent. This court has stated that "licenses are considered as nothing more than a promise by the licensor not to sue the licensee." *Jim Arnold Corp. v.*

Hydrotech Sys., Inc., 109 F.3d 1567, 1577, 42 USPQ2d 1119, 1127 (Fed. Cir. 1997). The covenant not to sue in paragraph 2.2 does not grant a transferable license to the patent.

CONCLUSION

Therefore, we vacate the district court's grant of summary judgment of non-infringement, generally affirm the district court's grant of summary judgment that Symantec did not license the '*776* Patent prior (but without limiting our holding to the period before March 2, 1999), and remand for further proceedings consistent with this opinion.

AFFIRMED-IN-PART, VACATED-IN-PART, AND REMANDED.

COSTS

No costs.

Appendix A

UNITED STATES COURT OF APPEALS
FOR THE FEDERAL CIRCUIT

00-1373, 00-1374

HILGRAEVE CORPORATION,

Plaintiff-Appellant,

v.

SYMANTEC CORPORATION,

Defendant-Cross Appellant.

JUDGMENT

ON APPEAL from the United States District Court for the Eastern District of Michigan

in CASE NO(S). 97-CV-40370

This CAUSE having been heard and considered, it is

ORDERED and ADJUDGED:

AFFIRMED-IN-PART, VACATED-IN-PART, AND REMANDED

Appendix A

ENTERED BY ORDER OF THE COURT

s/ Jan Horbaly
Jan Horbaly, Clerk

DATED SEP 17, 2001

APPENDIX B — MEMORANDUM OPINION AND ORDER DECIDED MARCH 28, 2000 AND FILED MARCH 29, 2000

HILGRAEVE CORPORATION,

Plaintiff,

v.

SYMANTEC CORPORATION,

Defendant.

CIVIL CASE NO. 97-40370

UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF MICHIGAN, SOUTHERN DIVISION

90 F. Supp. 2d 850; 2000 U.S. Dist. LEXIS 4120

March 28, 2000, Decided

March 29, 2000, Filed

JUDGES:

HONORABLE PAUL V. GADOLA, UNITED STATES DISTRICT JUDGE

* * *

Appendix B

MEMORANDUM OPINION AND ORDER GRANTING DEFENDANT'S MOTION FOR SUMMARY JUDGMENT OF NON-INFRINGEMENT

Among the many motions before this Court is Defendant Symantec Corporation's Motion for Summary Judgment of Non-Infringement filed September 14, 1999. For reasons stated below, this Court grants Defendant's motion, dismisses this civil action, and denies all other pending motions without prejudice as moot.

In support its Motion for Summary Judgment of Non-Infringement, Defendant submitted an opinion by Judge Nancy G. Edmunds in *Hilgraeve Corp. v. McAfee Associates, Inc.*, 70 F. Supp.2d 738 (E.D. Mich. 1999), issued on June 10, 1999. Judge Edmunds' opinion concerns the same patent, same patent claims, and same Plaintiff patentee alleging infringement by a party whose accused product is very similar to Defendant's in the instant case. The Complaints in her case and the instant case were filed on the same day, September 15, 1997. Plaintiff did not identify any companion case on the Civil Cover Sheets accompanying the Complaints, which helps explain why the relatedness of the cases was not discovered sooner. The two cases are, in effect, companion cases. *See* E.D. Mich. LR 83.11(b)(7)(A). The Memorandum Opinion and Order in *McAfee Associates* is on appeal to the United States Court of Appeals for the Federal Circuit; it also has some collateral estoppel effect on the instant case and, to the extent that it does not, this Court grants Defendant's Motion for Summary Judgment of Non-Infringement for the reasons similar to those stated in Judge Edmunds' opinion.

Appendix B

Factual and Procedural Background

Plaintiff is Hilgraeve Corporation, a Michigan corporation that owns U.S. Patent No. 5,319,776 (the " '*776* Patent"), the patent at issue in this civil action. The '*776 Patent*, entitled "In Transit Detection of Computer Virus With Safeguard," issued on June 7, 1994 to inventors John K. Hile, Matthew H. Gray, and Donald L. Wakelin and was thereafter assigned to Plaintiff. Defendant is Symantec Corporation, a Delaware corporation with its principal place of business in California.

On September 15, 1997, Plaintiff filed the instant action, alleging in a single Count that Defendant's products infringe *the '776 Patent* pursuant to Title 28, United States Code, Section 271. In the course of litigation, Plaintiff has alleged that nine of Defendant's products infringe the '*776* Patent: (1) pcANYWHERE, (2) Norton AntiVirus for Windows 95/98, (3) Norton AntiVirus for Windows NT, (4) Norton AntiVirus for Windows 3.X, (5) Norton AntiVirus for DOS, (6) Norton AntiVirus for Lotus Notes, (7) Norton AntiVirus for Netware, (8) Norton AntiVirus for E-Mail Gateways, and (9) Norton AntiVirus for Firewalls.

Defendant filed a counter-claim on December 30, 1997, alleging that the '*776 Patent* is invalid (Count I) and that Defendant did not infringe the '*776* Patent (Count II). Non-expert discovery closed on May 7, 1999, and expert discovery closed on August 6, 1999. Defendant now moves for summary judgment on Count II of its counter-claim.

Appendix B

Discussion

1. Standard for summary judgment

Rule 56 of the Federal Rules of Civil Procedure provides that summary judgment "shall be rendered forthwith if the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(c). Summary judgment is appropriate where the moving party demonstrates that there is no genuine issue of material fact as to the existence of an essential element of the nonmoving party's case on which the nonmoving party would bear the burden of proof at trial. *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986); *Martin v. Ohio Turnpike Commission*, 968 F.2d 606, 608 (6th Cir. 1992).

In considering a motion for summary judgment, the Court must view the facts and draw all reasonable inferences therefrom in a light most favorable to the nonmoving party. *60 Ivy Street Corp. v. Alexander*, 822 F.2d 1432, 1435 (6th Cir. 1987). The Court is not required or permitted, however, to judge the evidence or make findings of fact. *Id.* at 1435-36. The moving party has the burden of showing conclusively that no genuine issue of material fact exists. *Id.* at 1435.

A fact is "material" for purposes of summary judgment where proof of that fact would have the effect of establishing or refuting an essential element of the cause of action or a

defense advanced by the parties. *Kendall v. Hoover Co.*, 751 F.2d 171, 174 (6th Cir. 1984). A dispute over a material fact is genuine "if the evidence is such that a reasonable jury could return a verdict for the nonmoving party." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). Accordingly, where a reasonable jury could not find that the nonmoving party is entitled to a verdict, there is no genuine issue for trial and summary judgment is appropriate. *Id.*; *Feliciano v. City of Cleveland*, 988 F.2d 649, 654 (6th Cir. 1993).

Once the moving party carries its initial burden of demonstrating that no genuine issues of material fact is in dispute, the burden shifts to the nonmoving party to present specific facts to prove that there is a genuine issue for trial. To create a genuine issue of material fact, the nonmoving party must present more than just some evidence of a disputed issue. As the United States Supreme Court has stated:

> There is no issue for trial unless there is sufficient evidence favoring the nonmoving party for a jury to return a verdict for that party. If the [nonmoving party's] evidence is merely colorable, or is not significantly probative, summary judgment may be granted.

Anderson, 477 U.S. at 249-50 (citations omitted); *see Celotex*, 477 U.S. at 322-23; *Matsushita Electric Industrial Co., Ltd. v. Zenith Radio Corp.*, 475 U.S. 574, 586-87 (1986). Consequently, the nonmoving party must do more than raise some doubt as to the existence of a fact; the nonmoving party must produce evidence that would be sufficient to require submission of the issue to the jury. *Lucas*

v. Leaseway Multi Transportation Service, Inc., 738 F. Supp. 214, 217 (E.D. Mich. 1990), *aff'd*, 929 F.2d 701 (6th Cir. 1991). "The mere existence of a scintilla of evidence in support of the plaintiff's position will be insufficient; there must be evidence on which the jury could reasonably find for the plaintiff." *Anderson*, 477 U.S. at 252; *see Cox v. Kentucky Department of Transportation*, 53 F.3d 146, 150 (6th Cir. 1995).

2. Collateral estoppel

In general, the doctrine of collateral estoppel provides that when an issue of ultimate fact has been determined by a valid and final judgment, that issue cannot be litigated again in any future lawsuit involving the same parties. In some cases, a party that was not before the court for a prior judgment may benefit from that judgment in a future proceeding. According to the United States Court of Appeals for the Federal Circuit,

> A second defendant is entitled to the benefit of a judgment issued against the plaintiff in favor of a first defendant in prior litigation on the same issues. . . . [W]here a determination of the scope of patent claims was made in a prior case, and the determination was essential to the judgment there on the issue of infringement, there is collateral estoppel in a later case on the scope of such claims, i.e., the determined scope cannot be changed.

Molinaro v. Fannon/Courier Corp., 745 F.2d 651, 655 (Fed. Cir. 1984) (citing *A.B. Dick Co. v. Burroughs Corp.*, 713 F.2d 700 (Fed. Cir. 1983)); *see Pfaff v. Wells Electronics, Inc.*, 5 F.3d 514, 518 (Fed. Cir. 1993) ("The prior claim interpretation has issue preclusive effect in the present case insofar as it was necessary to the judgment of non-infringement in the previous case.").

The defendant's motion for summary judgment in *A.B. Dick Co. v. Burroughs Corp.*, 713 F.2d 700 (Fed. Cir. 1983), was grounded on the collateral estoppel effect of **another** court's holding that **another** defendant did not infringe the **same** patent. The Federal Circuit held that, "judicial statements regarding the scope of patent claims are entitled to collateral estoppel effect in a subsequent infringement suit only to the extent that determination of scope was essential to a final judgment on the question of validity or infringement; further, that such statements should be narrowly construed." *A.B. Dick*, 713 F.2d at 704.

Some issues in the instant case are **identical** to those adjudicated by Judge Edmunds in *McAfee Associates*, such as the proper construction of claims 1 and 18 of the *'776* Patent and the application of prosecution history estoppel to the doctrine of equivalents analysis. These issues can be resolved regardless of who the defendant may be since they concern the intrinsic evidence surrounding the patent. Here, as in *Molinaro* and *A.B. Dick,* the identical issues were decided previously, those issues were fully litigated in a previous case, the resolution of those issues was essential to a final judgment there, and the patent owner had a full and fair opportunity to litigate those issues. Therefore, the proper

construction of claims 1 and 18 of the '*776 Patent* and application of prosecution history estoppel to the doctrine of equivalents analysis in *McAfee Associates* has preclusive effect here.

3. Analysis

Determining patent infringement is a two-step process of (1) claim construction, and (2) claim comparison. *Hilgraeve Corp. v. McAfee Associates, Inc.*, 70 F. Supp.2d 738, 742 (E.D. Mich. 1999). In the first step, the Court must construe the meaning and scope of the disputed claim language. This step is considered a question of law, *see, e.g., Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 981 (Fed. Cir. 1995), and, therefore, is well suited for summary judgment. *McAfee Associates*, 70 F. Supp.2d at 742. In the second step, the Court must compare the properly construed claims with the accused product to determine whether the patent has been infringed either literally or under the doctrine of equivalents. *Wolverine World Wide, Inc. v. Nike, Inc.*, 38 F.3d 1192, 1200 (Fed. Cir. 1994); *McAfee Associates*, 70 F. Supp.2d at 742.

a. Claim construction

Since the proper construction of claims 1 and 18 of the '*776 Patent* is the identical issue previously adjudicated in *McAfee Associates*, and because this issue can be determined regardless of the particular defendant before the Court, the claim construction provided by Judge Edmunds has collateral estoppel effect to the extent that the determination of the scope of the '*776* Patent claims was essential to a final

judgment on the question of non-infringement. *See Pfaff v. Wells Electronics, Inc.*, 5 F.3d 514, 518 (Fed. Cir. 1993); *Molinaro v. Fannon/Courier Corp.*, 745 F.2d 651, 655 (Fed. Cir. 1984); *A.B. Dick Co. v. Burroughs Corp.*, 713 F.2d 700 (Fed. Cir. 1983). Therefore, this Court adopts Judge Edmunds' opinion on claim construction and only will summarize the relevant analysis below.

In the claim construction step, the Court must consider three kinds of intrinsic evidence: (1) the patent claims, (2) the patent specification, and (3) the prosecution history, if it is in evidence. *See e.g., Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996); *Markman*, 52 F.3d at 979; *McAfee Associates*, 70 F. Supp.2d at 742. First, in construing the language of the **patent claims,** the Court must give the words their "ordinary and customary meanings" unless the patentee has given the terms special definitions as "clearly stated in the patent specification or file history." *Vitronics Corp.*, 90 F.3d at 1582; *see McAfee Associates*, 70 F. Supp.2d at 742. Second, the **patent specification** is the written description of the invention and "may act as a sort of dictionary, which explains the invention and may define terms used in the claims." *Markman*, 52 F.3d at 979; *see Vitronics Corp.*, 90 F.3d at 1582; *McAfee Associates*, 70 F. Supp.2d at 742. A claim construction should include the preferred embodiment set forth in the patent specification, *see Hoeschst Celanese Corp. v. BP Chemicals Ltd.*, 78 F.3d 1575, 1581 (Fed. Cir. 1996), although the preferred embodiment does not necessarily limit the scope of a claim, *see Transmatic, Inc. v. Gulton, Industries, Inc.*, 53 F.3d 1270, 1277 (Fed. Cir. 1995). *See McAfee Associates*, 70 F. Supp.2d at 742. Third, the **prosecution history,** if in evidence,

"limits the interpretation of claim terms so as to exclude any interpretation that was disclaimed during prosecution," *Southwall Technologies, Inc. v. Cardinal IG Co.*, 54 F.3d 1570, 1576 (Fed. Cir. 1995), but it may not "enlarge, diminish, or vary the limitations in the claim." *Markman*, 52 F.3d at 980 (quotation omitted); *see McAfee Associates*, 70 F. Supp.2d at 743.

If the meaning and scope of a claim is clear after considering the language of the patent claims, the patent specification, and the prosecution history, then the Court should not consider any extrinsic evidence. *See Vitronics Corp.*, 90 F.3d at 1583; *McAfee Associates*, 70 F. Supp.2d at 743. If, however, the meaning and scope of a claim remains unclear, then the Court may consider extrinsic evidence "including expert and inventor testimony, dictionaries, and learned treatises." *Markman*, 52 F.3d at 980; *McAfee Associates*, 70 F. Supp.2d at 742.

In the instant case, Plaintiff accuses Defendant of infringing claims 1, 2, 6, 12, 14, 16, and 18 of the *'776 Patent*. Claims 1 and 18 are independent claims, whereas claims 2, 6, 12, 14, and 16 are dependent upon claim 1. A finding that Defendant's accused products do not infringe the independent claims will dispose of Plaintiff's case. *See Desper Products, Inc. v. OSound Labs, Inc.*, 157 F.3d 1325, 1338 n. 5 (Fed. Cir. 1998); *London v. Carson Pirie Scott & Co.*, 946 F.2d 1534, 1539 (Fed. Cir. 1991); *McAfee Associates*, 70 F. Supp.2d at 744. Therefore, the Court need concern itself only with claims 1 and 18.

Appendix B

Claim 1 reads as follows:

1. In a system for transferring digital data for storage in a computer storage medium, a method of screening the data *as it is being transferred* and automatically inhibiting the storage of screened data containing at least one predefined sequence, comprising the steps of:

causing a quantity of digital data resident on a source storage medium to be transferred to a computer system having a destination storage medium;

receiving and screening the transferred digital data prior to storage on the destination storage medium to determine if at least one of a plurality of predefined sequences are present in the digital data received; and

in response to said screening step:

(a) automatically causing the screened digital data to be stored on said destination storage medium if none of the plurality of predefined sequences are present and

(b) automatically inhibiting the screened digital data from being stored on said destination storage medium if at least one predefined sequence is present.

('*776* Patent, column 17, lines 9-29 (emphasis added).)

Appendix B

Claim 18 reads as follows:

> 18. A method of preventing the spread of computer viruses to a computer having a storage medium, comprising the steps of:
>
> *simultaneously searching* for a plurality of virus signatures, each of which comprising an identifiable digital sequence, *while said computer is receiving a stream of digital data for storage* on said storage medium;
>
> providing an indication of the detection of a virus from said searching step; and
>
> automatically inhibiting the storage of said digital stream on said storage medium if any of said virus signatures have been detected.

('*776 Patent*, column 18, lines 45-57 (emphasis added).)

As Judge Edmunds explained, "[c]laims 1 and 18 teach that virus screening or searching is done while incoming digital data is being received or transferred and before it is stored on the destination storage medium." *McAfee Associates*, 70 F. Supp.2d at 746. Claim 1 discloses that incoming digital data is first screened for viruses while the digital data is being received and "prior to storage on the destination storage medium," and then, "in response to said screening step," the "screened digital data" is either automatically "stored on the destination storage medium" if a virus is not detected or automatically inhibited from "being

stored on said destination storage medium" if one is detected during the screening step. Claim 18 discloses simultaneous searches for "a plurality of virus signatures . . . while said computer is receiving a stream of digital data for storage," and then, if a virus is detected "from said searching step," the '*776* Patent invention "automatically inhibit[s] the storage of said digital stream on said storage medium."

Judge Edmunds concluded that the term "storage" used in claims 1 and 18 required some clarification. Plaintiff had urged the *McAfee Associates* Court to recognize that "storage occurs 'when the incoming file or data is sufficiently present on the destination disk medium so any viruses can spread and infect the system.' " *McAfee Associates*, 70 F. Supp.2d at 745 n.7. The defendant in that case had asserted that "storage occurs 'when the digital data is written to, and present on, the destination medium, and accessible by the operating system or other programs, so any viruses contained in the data can spread elsewhere in the computer system.' " *Id.* Judge Edmunds noted that "[t]he parties essentially agree on the meaning of storage," *id.* at 745, and concluded that, "storage occurs when the incoming digital data is sufficiently present on the destination storage medium, and accessible by the operating system or other programs, so that any viruses contained in the data can spread and infect the computer system." *Id.*

Defendant here, in effect, urges this Court to delete from this definition the requirement that data must be "accessible by the operating system or other programs" in order to be considered stored. (*See* Def. Br. at 14-15.) Defendant argues that "[b]ecause claim interpretation is a question of law, . . .

a claim should not be interpreted based on an agreement by the parties in a related, but different, case." (*Id.* at 15.) While the "related, but different, case" to which Defendant refers has preclusive effect on this Court's claim interpretation, as explained above, this Court agrees that proper claim interpretation may not be based solely on the agreement of the parties.

As explained above, when construing patent claims, this Court is required to consider only the intrinsic evidence of the patent claims, the patent specification, and the prosecution history, unless the meaning and scope of those claims are unclear. Furthermore, while the Court is not required to adopt the meaning proffered by one or more of the parties, *see Exxon Chemical Patents, Inc. v. Lubrizol Corp.*, 64 F.3d 1553, 1555 (Fed. Cir. 1995), a party should not be permitted to argue for a different definition than the one it successfully urged the court below to adopt. Therefore, in light of there being no apparent requirement in claims 1 or 18, the patent specification, or the prosecution history that the stored data be "accessible by the operating system or other programs," and Plaintiff having argued below that "storage" occurs "when the incoming file or data is sufficiently present on the destination disk medium so any viruses can spread and infect the system," this Court will construe "storage" here as follows: storage occurs when the incoming digital data is sufficiently present on the destination storage medium so that any viruses contained in the data can spread and infect the computer system. By omitting from the definition a restriction that does not have a basis the patent claims, patent specification, or prosecution history, this definition is closer

to the ordinary and customary meaning of the term in this context and still appears to be consistent with the definitions offered by the parties' experts.

According to the patent specification, the invention receives part of the incoming digital data in a buffer during the data transfer. *McAfee Associates*, 70 F. Supp.2d at 748. The invention scans the data in the buffer for the presence of a predefined digital sequence, such as a virus signature, before storing the data on the destination medium. *Id.* If a predefined sequence is found in the digital data, the data in the buffer is inhibited from being stored on the destination storage medium. *Id.* If a predefined sequence is not found in the digital data, the data is then transferred from the buffer to a file on the destination storage medium where it is then stored. *Id.* If a predefined sequence is subsequently detected in an incoming block of digital data, the previously stored, virus-free block of digital data can be purged or overwritten as an added anti-virus safety. *Id.*

In the preferred embodiment, the "string search routine" disclosed in the '*776* Patent tests each character within a block of data as it enters the buffer by searching for a match to a virus signature. ('*776 Patent*, column 5, lines 2-21.) *See McAfee Associates*, 70 F. Supp.2d at 747. A block of data is transmitted, screened for viruses, and stored in a file if it is virus-free, and then the next block of data is transferred, and the process is repeated. ('*776 Patent* column 6, lines 22-68; column 7, lines 1-14.) *See McAfee Associates*, 70 F. Supp. 2d at 747. If, in response to the screening step, a virus is detected in a block of data being transmitted, the transfer is canceled prematurely, (*id.* column 6, lines 14-16),

and the data in the file can be purged or deleted by overwriting, (*id.* column 6, lines 24-31). *See McAfee Associates*, 70 F. Supp.2d at 747.

Finally, the prosecution history shows that "prior to storage on the destination storage medium" was added to distinguish the '*776 Patent* invention from the prior art. *See McAfee Associates*, 70 F. Supp.2d at 748.

b. Claim comparison

i. Literal infringement

To establish that Defendant's accused product literally infringe Plaintiff's '*776* Patent, every limitation of claims 1 and 18 must be found in Defendant's accused products. *See London v. Carson Pirie Scott & Co.*, 946 F.2d 1534, 1539 (Fed. Cir. 1991). ("There can be no infringement as a matter of law if a claim limitation is totally missing from the accused device."). "[A] literal infringement issue is properly decided upon summary judgment when no genuine issue of material fact exists, in particular, when no reasonable jury could find that every limitation recited in the properly construed claim either is or is not found in the accused device." *Bai v. L & L Wings, Inc.*, 160 F.3d 1350, 1353 (Fed. Cir. 1998); *see McAfee Associates*, 70 F. Supp.2d at 751.

In order to determine whether the accused products literally infringe the '*776* Patent, the Court must compare the claim constructions above with Defendant's accused products. *McAfee Associates*, 70 F. Supp.2d at 751. As in *McAfee Associates*, Plaintiff asserts that Defendant's accused

products infringe claims 1 and 18 because they screen incoming digital data for viruses during transfer and before storage on the destination storage medium. *Id.* Defendant asserts the accused products screen for viruses only after all the incoming digital data has been transferred and stored on the destination storage medium. According to Defendant, none of its accused products "screen [] the data as it is being transferred," "screen[] the transferred digital data prior to storage on the destination storage medium," or "in response to said screening steps . . . automatically caus[e] the screened digital data to be stored on said destination storage medium" as required by claim 1, nor do they "search[] for a plurality of virus signatures . . . while said computer is receiving a stream of digital data for storage on said storage medium" as required by claim 18. This Court agrees.

Each of Defendant's accused products generally operates as follows. First, a file is transferred for storage on the destination storage medium. (Melvin Decl. ¶ 6.) This transfer includes opening a new file on the destination storage medium, transferring data to that medium, and recording the data into the new file. (*Id.*) Second, the application causing the transfer makes a request to the operating system to close the file containing the transferred data. (*Id.*) Third, the operating system closes the file. (*Id.*) After the operating system closes a file, the file is recorded on the storage medium and the file is accessible to the operating system and to other application programs. (*Id.* ¶ 9.) Fourth, after the file is closed, the accused products invoke the Norton AntiVirus Scan Engine in order to test the file for the presence of a computer virus. (*Id.* ¶ 6.) The transferred file is accessible to other programs prior to being examined by the accused products

because the Norton AntiVirus Scan Engine is not invoked and does not access the transferred file until after the operating system closes the file. (*Id.* ¶ 9.) To invoke the Norton AntiVirus Scan Engine, the file to be scanned must be completely received and stored on the local disk drive, the file must be closed, and the file name of the closed file must be given to the Norton AntiVirus Scan Engine. (Id. ¶ 7.) In short, the accused products scan for viruses only after the entire file has been transferred and after the file has been stored on the destination storage medium. *Compare McAfee Associates*, 70 F. Supp.2d at 752.

There apparently is no dispute between the parties regarding the manner in which the accused products operate. Referring to Defendant's "Statement of Undisputed Facts," Plaintiff states that "the parties agree that there is no dispute about how the products operate." (Pl.'s Br. at 4.) Furthermore, Plaintiff's expert repeatedly states that he agrees with Defendant's expert about how Defendant's products work. (*See* Magen Decl. Ex. 19 (Geske Report), at 7, 9, 12, 14, 15, 16.) Defendant's summary of how its products operate as presented in the "Statement of Undisputed Facts" was gleaned from Defendant's expert. (*See, e.g.*, Def.'s Br. at 8.)

The accused products first allow the incoming digital data to be stored as a whole on the destination storage medium before it is scanned. Virus screening is performed only after the incoming digital data has been fully transferred and stored. Therefore, the accused products cannot perform the "receiving and screening . . . prior to storage" limitation of claim 1 or the "searching for . . . virus signatures . . . while said computer is receiving a stream of digital data for storage

on said storage medium" as required by claim 18. Because there is no dispute about how the accused products operate, there is no genuine issue as to any material fact concerning whether Defendant's accused products literally infringe the '*776* Patent. Accordingly, because every limitation of claims 1 and 18 are not found in the accused products, this Court may grant summary judgment on the question of whether the accused products do not literally infringe the '*776* Patent.

ii. Doctrine of equivalents

According to the doctrine of equivalents, "a product or process that does not literally infringe upon the express terms of a patent claim may nonetheless be found to infringe if there is 'equivalence' between the elements of the accused product or process and the claimed elements of the patented invention." *Warner-Jenkinson Co. v. Hilton Davis Chemical, Co.*, 520 U.S. 17, 21 (1997); *McAfee Associates*, 70 F. Supp.2d at 757. The Supreme Court concluded that whatever approach is used for determining equivalence — e.g., the triple identity or the insubstantial differences approach—it must be "probative of the essential inquiry: Does the accused product or process contain elements identical or equivalent to *each claimed element* of the patented invention?" *Warner-Jenkinson*, 520 U.S. at 40 (emphasis added); *see McAfee Associates*, 70 F. Supp.2d at 757.

The determination of equivalence "must be applied to individual elements of the claim, not to the invention as a whole," *Warner-Jenkinson*, 520 U.S. at 29, and "should be applied as an objective inquiry on an element-by-element basis," *id.* at 40. *See McAfee Associates*, 70 F. Supp.2d

at 757. The Court must focus on individual elements with "a special vigilance against allowing the concept of equivalence to eliminate completely any such elements." *Warner-Jenkinson*, 520 U.S. at 40; *see McAfee Associates*, 70 F. Supp.2d at 757. "[A]pplication of the doctrine, even as to an individual element, is not allowed such broad play as to effectively eliminate that element in its entirety." *Warner- Jenkinson*, 520 U.S. at 29; *see McAfee Associates*, 70 F. Supp.2d at 757. "An analysis of the role played by each element in the context of the specific patent claim will thus inform the inquiry as to whether a substitute element matches the function, way, and result of the claimed element, or whether the substitute element plays a role substantially different from the claimed element." *Warner-Jenkinson*, 520 U.S. at 40, 117 S. Ct. 1040; *see McAfee Associates*, 70 F. Supp.2d at 757.

As in *McAfee Associates*, Defendant contends that prosecution history estoppel precludes Plaintiff from asserting a claim of infringement under the doctrine of equivalents. *See McAfee Associates*, 70 F. Supp.2d at 757. Since the effect of prosecution history is the same as that considered in *McAfee Associates*, and because what Plaintiff may be estopped from arguing on account of that prosecution history can be determined regardless of the particular defendant before the Court, the analysis of prosecution history estoppel provided by Judge Edmunds has collateral estoppel effect to the extent that the effect of the prosecution history was essential to a final judgment on the question of non-infringement. *See Pfaff v. Wells Electronics, Inc.*, 5 F.3d 514, 518 (Fed. Cir. 1993); *Molinaro v. Fannon/Courier Corp.*, 745 F.2d 651, 655 (Fed. Cir. 1984); *A.B. Dick Co. v.*

Burroughs Corp., 713 F.2d 700 (Fed. Cir. 1983). Therefore, this Court adopts Judge Edmunds' analysis of prosecution history estoppel as summarized below.

Prosecution history estoppel is an established limitation on the doctrine of equivalents. As the Federal Circuit explained in *Bai v. L & L Wings, Inc.*, "[a]n applicant who responds to an examiner's prior art rejection by narrowing his claim cannot later assert that the surrendered subject matter is an equivalent of the amended limitation." 160 F.3d at 1356; see *Warner-Jenkinson Co.*, 520 U.S. at 33 (amending claims during prosecution creates a presumption of prosecution history estoppel); *McAfee Associates*, 70 F. Supp.2d at 758. The purpose of prosecution history estoppel is to prevent a patentee from obtaining, through litigation, coverage of subject matter surrendered during prosecution in order to gain acceptance of a claim. *See Haynes International, Inc. v. Jessop Steel Co.*, 8 F.3d 1573, 1577-78 (Fed. Cir. 1993), *modified on rehearing*, 15 F.3d 1076 (Fed. Cir. 1994) (affirming summary judgment of non-infringement); *McAfee Associates*, 70 F. Supp.2d at 757. Prosecution history estoppel is a question of law for the Court and, therefore, is suitable for summary judgment. *See Bai*, 160 F.3d at 1356 (affirming summary judgment of non-infringement because of prosecution history estoppel); *McAfee Associates*, 70 F. Supp.2d at 757.

The legal standard for determining prosecution history estoppel is "an objective one, measured from the vantage point of what a competitor was reasonably entitled to conclude, from the prosecution history, that the applicant

gave up to procure issuance of the patent." *Haynes International*, 8 F.3d at 1578; *see McAfee Associates*, 70 F. Supp.2d at 757-58.

If "a patent applicant has made a substantive change to his claim that clearly responds to an examiner's rejection of that claim as unpatentable over prior art, prosecution history estoppel applies to that claim; only the question of the scope of the estoppel remains." *Sextant Avionique, S.A. v. Analog Devices, Inc.*, 172 F.3d 817, 826 (Fed. Cir. 1999); *Bai*, 160 F.3d at 1355; *see McAfee Associates*, 70 F. Supp.2d at 758. "The scope of the estoppel . . . includes features that the applicant amended his claim to avoid or trivial variations of such prior art features. Moreover, prosecution history estoppel cannot be avoided by filing a continuing application with narrowed claims rather than responding directly to an outstanding rejection." *Desper Products*, 157 F.3d at 1338 (quotations omitted); *see McAfee Associates*, 70 F. Supp.2d at 758. The scope of the estoppel is ascertained by considering the subject matter surrendered during the prosecution history and "is determined with reference to the prior art and any amendments and/or arguments made in an attempt to distinguish such art." *Sextant Avionique*, 172 F.3d at 827 (citations omitted); *see McAfee Associates*, 70 F. Supp.2d at 758.

Here, claims 1 and 18 were originally submitted with no limitation that virus screening was to be performed "prior to storage." (*See* Magen Decl. Ex. 3.) *See McAfee Associates*, 70 F. Supp.2d at 758. In response to the Patent and Trademark Office's rejection of the original application, "the applicants

amended the patent claims and argued that the claims were patentable because they required that virus screening be performed during the transfer of incoming digital data and before storage." *McAfee Associates*, 70 F. Supp.2d at 758. (*See* Magen Decl. Ex. 8.)

The prosecution history shows that the applicants narrowed the scope of claims 1 and 18 to avoid the prior art by adding the limitation that virus screening was to be performed "prior to storage on the destination storage medium," and thereby surrendering methods that screen for viruses after storage. *McAfee Associates*, 70 F. Supp.2d at 758. As a result of these amendments, a competitor was reasonably entitled to conclude that the applicants gave up methods that screen for viruses after storage in order to procure issuance of the '*776* Patent. Therefore, as in *McAfee Associates,* Plaintiff "is estopped from arguing here that the accused product[s], which screen[ ] for viruses after 'storage,' infringe[] any claim of the '*776* Patent under the doctrine of equivalents." *See McAfee Associates*, 70 F. Supp.2d at 758. As discussed above, Defendant's accused product scans for viruses after storage. Therefore, this Court may grant summary judgment that the accused products do not infringe the '*776* Patent under the doctrine of equivalents.

Conclusion

Accordingly, this Court being fully advised in the premises,

Appendix B

IT IS HEREBY ORDERED that Defendant's Motion for Summary Judgment of Non- Infringement [Docket Entry 149] is **GRANTED.**

IT IS FURTHER ORDERED that this civil action is **DISMISSED.**

IT IS FURTHER ORDERED that all other pending motions are **DENIED** without prejudice as moot.

SO ORDERED.

Dated: 3/28/00

s/ Paul v. Gadola
HONORABLE PAUL V. GADOLA
UNITED STATES DISTRICT JUDGE

APPENDIX C — ORDER OF THE UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT DENYING PETITION FOR REHEARING DATED AND FILED NOVEMBER 6, 2001

UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT

ORDER

A combined petition for panel rehearing and for rehearing en banc having been filed by the CROSS-APPELLANT, and the petition for rehearing having been referred to the panel that heard the appeal, and thereafter the petition for rehearing en banc having been referred to the circuit judges who are in regular active service,

UPON CONSIDERATION THEREOF, it is

ORDERED that the petition for panel rehearing be, and the same hereby is, DENIED and it is further

ORDERED that the petition for rehearing en banc be, and the same hereby is, DENIED.

The mandate of the court will issue on November 13, 2001.

FOR THE COURT

s/ Jan Horbaly
Jan Horbaly
Clerk

Dated: November 6, 2001

cc: Ernie L. Brooks
Martin C. Fliesler